



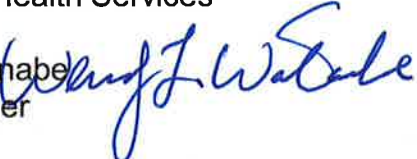
**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

July 17, 2013

TO: Mitchell H. Katz, M.D., Director
Department of Health Services

FROM: Wendy L. Watanabe 
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW – LAC+USC
MEDICAL CENTER**

We have completed a review of the Department of Health Services (DHS) Los Angeles County + University of Southern California Medical Center's (LAC+USC) compliance with the Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic Clinical Health (HITECH) Act.¹ On May 3, 2013, we provided your Department with our final draft report, and conducted an exit conference on July 9, 2013. At the exit conference, your Audit and Compliance Division indicated that they will issue a response in 30 days.

Approach/Scope

The purpose of the review was to evaluate LAC+USC's compliance with HIPAA and the HITECH regulations, including best practices and relevant County and Departmental policies and procedures. The scope of this review included the *HIPAA Privacy Rule and HITECH Act Audit Tool*, which is a general assessment to determine whether the LAC+USC is compliant with privacy, security, training, policies and procedures, and breach notification requirements. During the course of the review, we expanded our scope to include Health Services Administration's (HSA) efforts to implement the Department's HIPAA program at LAC+USC.

Our review covered the Privacy Rule requirements for: 1) notice of privacy practices for protected health information (PHI), 2) safeguards for privacy protections for PHI, 3) workforce member access to PHI, 4) administrative requirements, 5) disclosures of PHI, 6) amendment of PHI, 7) accounting of disclosures, and 8) the interim requirements for the HITECH Act's Breach Notification Rule.

¹ 45 Code of Federal Regulations (CFR) Parts 160 and 164

The review also covered certain areas of the Security Rule's policies for: 1) administrative, 2) physical, and 3) technical safeguards.

To assist us with this review, we met with representatives from HSA, DHS' Audit and Compliance Division, LAC+USC's Chief Medical Officer and staff, Information Technology (IT) Division managers and staff, and LAC+USC's Privacy Officer and Health Information Management personnel. In addition, the County's Chief Information Security Officer (CISO), Robert Pittman, reviewed DHS' responses applicable to the Security Rule.

Results of Review and Recommendations

Notice of Privacy Practices

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the Notice of Privacy Practices (NPP) to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy.²

Our review found that LAC+USC has a joint NPP with USC. The joint NPP is posted in all designated waiting areas where patients are likely to view it. The NPP is current and includes the correct information on patient HIPAA rights, as well as the contact information for the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and the County's Chief HIPAA Privacy Officer. Posting the NPP is crucial to promoting the awareness of HIPAA privacy rights related to services received at LAC+USC. It also satisfies the HIPAA Privacy Rule's physical posting of the NPP requirement.

In addition, the HIPAA Privacy Rule requires covered entities that maintain a website to prominently post their NPP on their website.³

We reviewed the LAC+USC website in July 2012, and noted that it included a link to its joint NPP with USC, in both English and Spanish. However, we had difficulty finding the link as it was in 8-point font and at the bottom of the patient information page.

Recommendation

- 1. DHS and LAC+USC management prominently post the link to its NPP on its website where it would be easier for patients to find it, and change**

² Ibid., §164.520(c)

³ Ibid.

the link from 8-point font to 12-point font. Additionally, we recommend that your Office send a memorandum to each DHS facility notifying their privacy coordinators to prominently post the NPP on their respective facility websites accordingly.

LAC+USC's response indicates that they implemented our recommendation and are compliant with the Notices of Privacy Practices' posting standards.

Notices of Privacy Practices Acknowledgement of Receipt

A covered health care provider with a direct treatment relationship with individuals is required to make a good faith effort to obtain an individual's acknowledgement of receipt of the notice only at the time the provider first gives the notice to the individual (i.e., at first service delivery).⁴

It appears that LAC+USC is compliant with the NPP Acknowledgement of Receipt standards. We randomly selected and reviewed 20 patients' medical charts to determine whether LAC+USC obtained patients' acknowledgement of receipt of the NPP. All charts reviewed included the acknowledgement of receipt documentation, except for a newborn's chart where the mother signed on behalf of the infant, and the acknowledgement was not required.

Physical Safeguards

A covered entity must have in place appropriate administrative and physical safeguards to protect the privacy of PHI. A covered entity must reasonably safeguard PHI and electronic PHI (ePHI), and make reasonable efforts to prevent any intentional or unintentional use or disclosure that is in violation of the Privacy Rule.

It appears that LAC+USC is compliant with the physical safeguards' standards that we reviewed. During the review, we found that computer monitors that were in public areas were positioned away from the public's view so that the information was not readable. Fax machines, printers, and copiers were kept in secure areas and away from visitors. The public did not have access to non-public areas of the hospital, outpatient clinic, and administrative offices. Visitors are escorted by a workforce member.

In addition, the medical records' room is located in the basement of the old hospital and only authorized workforce members have access to the area. This arrangement is in accordance with the HIPAA Privacy Rule and appropriate physical safeguards are met, and in compliance with the regulations.

⁴ Ibid., §164.520(c)(2)

Administrative Safeguards for PHI

HIPAA requires that covered entities have in place appropriate administrative, technical, and physical safeguards for PHI. Specific guidance as to what constitutes appropriate safeguards is provided in the Security Rule. However, the Privacy Rule, which extends to non-electronic information, does not define reasonable or appropriate. As such, in implementing reasonable safeguards, LAC+USC must analyze its needs and circumstances, such as the nature of the PHI, and assess the potential risks to patients' privacy.

During our review, we found that LAC+USC's pharmacy places patients' first initials and last names on a marquee located above the registration windows to notify patients that their medications are ready. LAC+USC and County Counsel analyzed the circumstances for the disclosure and determined that it is incidental. We concur.

Minimum Necessary Rule

The Privacy Rule requires covered entities to make reasonable efforts to limit the use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose of the disclosure. The OCR allows covered entities flexibility to address their unique circumstances, and make their own assessment of what PHI is reasonably necessary for a particular purpose.⁵ As of the date of this report, the minimum necessary standard does not apply to disclosures, including oral disclosures, among health care providers for treatment purposes.

It appears that DHS' current policy meets the HIPAA standard on the Minimum Necessary Rule. Discussions with DHS and LAC+USC management indicate that workforce members are aware of the minimum necessary standards and to the best of their ability they adhere to them. They are further aware that the standards do not apply in certain situations, such as for treatment or when disclosures are required by law. LAC+USC has a *Minimum Necessary* policy that provides procedures for non-routine requests to disclose PHI.

Training

A covered entity must train all members of its workforce on policies and procedures related to PHI that are required by the HIPAA Privacy and Security Rules, to the extent necessary and appropriate for the members of its workforce to carry out their functions. Members of the workforce include workforce members, volunteers, and trainees.⁶

During the review, we were informed that all LAC+USC workforce members have received training on HIPAA, the HITECH Act Breach Notification Rule, and DHS' HIPAA policies and procedures. New-hire training is handled by DHS' Human Resources

⁵ Ibid., § 164.502 and 514(d)

⁶ Ibid., § 164.530(b)

Division through the orientation process. Existing DHS and LAC+USC workforce members also receive classroom training, and are provided a HIPAA study guide that includes a multiple choice test. Upon the workforce member's completion of the study guide, DHS/LAC+USC manually documents that the workforce member received HIPAA training and logs it in a binder.

We reviewed LAC+USC's training records, and found that 94 (1.4%) out of 6,656 workforce members have not completed the required HIPAA training. DHS indicated that LAC+USC's Privacy Officer sends frequent reminders to delinquent workforce members. In addition, the HIPAA training will soon be offered to all DHS workforce members via the County's Learning Management System (LMS). DHS tailored their compliance training materials to be inclusive of all federal and State privacy, security, and patient safety regulations. However, at the time of this report, only new hires could complete DHS' HIPAA training via LMS.

While we are supportive of DHS' efforts to implement a comprehensive, LMS-based training, we noted the Department does not have a mechanism to update their training materials when laws change. DHS has indicated that they will provide supplemental classroom training and/or update the study guide, and provide it to workforce members whose duties may be impacted by the new or revised standards, during the annual performance evaluation process. However, the HIPAA Security Rule requires that all workforce members receive training, including management. Thus, DHS' solution may not be adequate.

Recommendation

- 2. DHS management develop a plan to direct workforce members to utilize the County's LMS HIPAA training materials until DHS' online training materials are updated, or DHS provides an acceptable alternative.**

DHS' response indicates that it has a plan to train workforce members on revised policies and procedures as a result of changes in federal and/or State law, such as staff meetings, administrative briefings, and electronic communications with attestations tracked by identification number.

Training Materials

In addition to the online training program, we reviewed DHS' HIPAA Privacy and Security Comprehensive Self-Study Guide (Guide), which was last revised on November 17, 2005. It is DHS' practice to provide a hardcopy of the Guide to workforce members who do not have access to the online training program. While a complete analysis of the Guide is beyond the scope of this review, we noted that the Guide has not been updated to reflect regulatory standards, and in some cases significantly misstates the law. Below are examples of our findings:

- The Guide states: “The term for protected health information (PHI) as defined in HIPAA means any information that is created or received by a health care provider, health plan, employer, life insurer, school or university”. This definition is misleading because the HIPAA definition of PHI excludes health information in education records covered by the Family Educational Rights and Privacy Act.
- The Guide does not address the HITECH breach reporting requirements for unsecured PHI. Section 13402 of the HITECH Act requires HIPAA covered entities and their business associates to notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, or disclosed as a result of such breach. Covered entities are required to provide workforce training on the Breach Notification Rule.
- Guide Section VII, *Reasonable Precautions*, states that “A physician or nurse may talk about a patient’s condition or treatment with the patient, family or other provider over the phone or in a shared treatment area”. This statement is misleading, and could result in a breach if the patient does not want his/her PHI discussed with anyone. 45 CFR §164.510(b) states that if the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient’s health information with a family member, friend, or other person *if the patient agrees or, when given the opportunity, does not object.* (Emphasis added).
- The Guide does not adequately address the restrictive regulations for substance abuse treatment programs. Generally, any release of PHI containing substance abuse information requires consent by the patient and/or the treating physician/therapist. This omission could lead to prohibited disclosures by workforce members that are not aware of the consent requirements.

We noted that DHS is transitioning from the Guide to comprehensive online Privacy and Confidentiality training. However, the Department could not provide a target date for full implementation. If DHS will continue using the guide, they should ensure it is updated.

Recommendation

- 3. DHS management update the Guide to incorporate HITECH Act standards, along with any other requirements that preempt HIPAA and the HITECH Act, and ensure compliance with the standards.**

DHS’ response indicates that their training does contain information on the HITECH Act’s Breach Notification Rule. DHS initiated transitioning the training from the Guide to the updated Privacy and Confidentiality training. The Guide will be removed upon full transition.

While we agree that the online training is compliant with HIPAA and the HITECH Act regulations, the Guide is not compliant. Workforce members trained solely from the Guide are not being educated on current standards and requirements. In addition, DHS' response did not address the issue that the Guide has not been updated since 2005, and the Department does not have a target date to transition all workforce members to the online training.

Complaint Process

A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures. A covered entity must document all complaints received, and their disposition, if any.⁷

According to the LAC+USC Privacy Officer, if a patient or visitor wants to file a complaint, they are directed to the Patients Rights' Office located in the main hospital, where the complainant receives a "Grievance Form". If the complainant needs assistance, Patients Rights' staff will fill out the complaint on his/her behalf. Complaints are forwarded to the facility's administrator, who will assess the complaint type (e.g., health and safety, privacy, security, or other), and attempt to resolve all complaints within ten days. If additional time is needed to resolve the complaints, patients will be contacted in writing.

In addition to having a complaint process, DHS' NPP states how and where an individual may file a complaint with DHS' Privacy Officer, the County's Chief HIPAA Privacy Officer, and/or OCR. It appears that LAC+USC has a complaint process that meets the HIPAA standards.

Refraining from Intimidating or Retaliatory Acts

Discussions with LAC+USC management confirm their awareness and understanding of the requirement to adhere to LAC+USC's non-retaliation policy. Further, they understand that OCR will investigate any complaint against a covered entity that engages in retaliatory actions. It appears that LAC+USC's Policy 203.6 *Non-retaliation* is compliant with the HIPAA retaliatory acts' standard.

Uses and Disclosures Requiring an Authorization

The OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the individual. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the use or disclosure, (3) the person to whom the covered entity may make the disclosure,

⁷ Ibid., §164.530(d)

(4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

Discussions with LAC+USC's management and Privacy Officer confirm that their workforce members have a general understanding of DHS' policy regarding uses and disclosures requiring an authorization from patients or their legal representatives. Our review of DHS' *Authorization for Use and Disclosure of Protected Health Information* form shows that it meets the HIPAA required elements. It appears that LAC+USC is compliant with the uses and disclosures requiring an authorization standard.

Accounting of Disclosures of PHI

An individual has a right to receive an accounting of disclosures of PHI made by a covered entity. Covered entities must account to individuals for certain non-routine disclosures of PHI, and the Privacy Rule allows individuals to receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, up to six years after the disclosure. Disclosures that are not required to be reported include: to the individual; for treatment, payment, and health care operations; for facility directories; pursuant to authorization; pursuant to a limited data set agreement; to persons involved in the individual's care; for correctional institutions; and, certain law enforcement purposes.

LAC+USC does not manually maintain an accounting of disclosures for patients. Instead, all disclosures are tracked systematically by the Affinity IT program. LAC+USC has never received a request for an accounting of disclosures since the Privacy Rule became effective in April 2003. It appears that LAC+USC is compliant with the accounting of disclosures of PHI standard.

HITECH Act Breach Notification

The HHS issued regulations requiring health care providers, health plans, and other entities covered by HIPAA to notify individuals when their health information is breached. These "breach notification" regulations implement provisions of the HITECH Act. The regulations, developed by the OCR, require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

We were initially informed by DHS and LAC+USC management that workforce members are required to follow DHS' Policy 361.11, *Investigation of Privacy-Related Complaints Involving Alleged Violations or Breaches of Protected Health Information (PHI)*, which provides procedures for workforce members when they encounter a potential privacy and/or security breach. However, on December 20, 2012, HSA

provided this Office with LAC+USC's policies that address the HITECH Act Breach Notification Rule and complaint and investigation procedures, along with other relevant policies. As such, our review covers both policies.

We noted that DHS Policy 361.11 combines investigation procedures, the complaint process, and instructions on how to report a breach in one document, and we believe it is convoluted. In addition, the policy does not highlight important terms, procedures, and concepts, such as breach notification, making compliance difficult for individual users.

In contrast, LAC+USC has four policies (203.7, 217, 415, and 466), covering compliance, investigation procedures, and the breach notification process, which makes it easier for staff to find the subject matter and comply. Policy 361.11 is not consistent with best practices concerning policy development.

Recommendation

4. HSA management revise Policy 361.11 to separately address how to file a complaint, investigation procedures, and the breach notification process.

DHS indicated that their Policy 361.11, Investigation of Privacy-Related Complaints Involving Alleged Violations or Breaches of PHI, is a system-wide policy that provides the overall infrastructure and procedures.

We continue to recommend that DHS revise policy 361.11 to present key information in a more clear and usable format.

Security Rule Requirements

A comprehensive Security Rule audit is beyond the scope of this review. However, we requested that LAC+USC and DHS provide written responses to specific questions related to their compliance with the Security Rule. We shared DHS' responses with the CISO, who found them satisfactory. We also reviewed applicable DHS Security Rule policies, and met with DHS and LAC+USC IT management. Based on this limited review, it appears that DHS' Security Policies meet the Security Rule standards.

Technical Safeguards

HIPAA requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI in any form.⁸ This means that DHS must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. In

⁸ Ibid., §164.530(c)

addition, the Security Rule requires that covered entities implement policies and procedures to address the final disposition of ePHI and/or the hardware of electronic media on which it is stored.⁹

LAC+USC and DHS have policies to safeguard PHI and ePHI. In addition, LAC+USC has a policy requiring that computers be password protected, and management indicated that systems controls have been put in place to require password changes every 90 days, and to automatically log users out after five minutes of inactivity. Workforce members are frequently reminded to protect their passwords, to not share their passwords with anyone, and to not store PHI on hard drives. Additionally, the level of access to patients' electronic medical records is determined and granted based on the workforce member's job.

Our review examined whether LAC+USC policies are compliant with the HIPAA and HITECH regulations. To the extent that we were able to review LAC+USC's technical safeguards policies, their policies appear to comply with the HIPAA and HITECH standards. We also reviewed the Auditor-Controller Audit Division's October 25, 2012 review of LAC+USC's compliance with Board of Supervisors IT and security policies.

Appropriate Access to ePHI

The Security Rule requires covered entities to have policies and procedures to ensure that workforce members have appropriate access to ePHI, and to prevent those workforce members who do not have access from obtaining access to ePHI.¹⁰

DHS Policy 935.15 *System Audit Controls* addresses controls to record and examine system activity for all electronic information systems. DHS stated that access to its applications require users to authenticate to the system, and that they maintain session logs, rights, and other tools to ensure appropriate access to the system's data. DHS Policy 935.14 *System Access Controls* addresses the requirement to preserve and protect the confidentiality, integrity, and availability of ePHI on DHS networks, systems, software programs, for those workforce members that have access rights.

According to DHS, current user accounts are established upon completion and approval of the required access request forms. However, DHS is in the process of merging DHS' directory services with the Countywide standard, MS Active Directory, which is hosted by the Internal Services Department. Upon completion, user accounts will be created for new workforce members in eCAPS. When a workforce member terminates service with DHS, the Department will process the appropriate forms to delete the member's account, and the user will no longer have network access.

While DHS and LAC+USC have the capacity to record a workforce member's access to ePHI, they do not have controls in place to limit access to the network once access has

⁹ Ibid., §164.310(d)

¹⁰ Ibid., §308(a)(3)(i)

been granted. In other words, LAC+USC's current Affinity Health Care System does not have the feature to limit access based on a workforce member's job duties, also known as role-based access. This is an addressable weakness, and overall LAC+USC's current practices appear to be compliant with the Security Rule. To the extent that we were able to review LAC+USC's Systems Controls' Policy, it appears they are compliant with this standard.

Contingency Plan

The Security Rule includes requirements for covered entities to ensure the confidentiality, integrity, and availability of all ePHI information they create, receive, maintain, or transmit. The Rule further requires that covered entities protect against any reasonably anticipated threats or hazards to the security or integrity of such information. Other provisions require policies and procedures for responding to emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI. Contingency plans must be implemented and tested.¹¹

DHS' Policy 935.07 *Facility IT Contingency Plan* details the requirements that LAC+USC must follow to be compliant with HIPAA regulations. In addition, DHS' and LAC+USC indicated that DHS built a new data center at the Martin Luther King, Jr., Multi-Service Ambulatory Care Center campus that will maintain DHS facility back-up computer applications. DHS is in the process of replacing the existing Federated Affinity Health Information System applications with a fault tolerant consolidated enterprise Affinity system. The new configuration includes redundant partitions, offsite data replication, and automated data back-up provisions. Further, as part of its disaster recovery plan, DHS contracts with a vendor who transports back-up tapes to a secure location. It appears that DHS' Policy 935.07 *Facility IT Contingency Plan* addresses the Security Rule standard.

Proper Destruction of PHI

Covered entities must implement reasonable safeguards to limit incidental and prohibited uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the Security Rule requires implementation of policies and procedures to address the final disposition of ePHI and/or the hardware and electronic media on which PHI is stored.¹²

DHS' Policy 935.13 *Device and Media Controls* addresses proper disposal of ePHI. The policy states that "prior to disposal or transfer of IT resources out of DHS' inventory, all information and software containing PHI shall be rendered unreadable and unrecoverable to prevent unauthorized disclosure of DHS data". It appears that DHS' Policy 935.13 *Device and Media Controls* is compliant with this standard.

¹¹ Ibid.

¹² Ibid., 164.310(d)(2) and 164.530(c)

Conclusion

We discussed our findings and recommendations with HSA and LAC+USC management on July 9, 2013. HSA indicated that they intend to provide a response in 30 days. Our recommendations address best practices' measures, specifically training, which takes into consideration the size of DHS, LAC+USC, workforce members exposed to PHI, staff turnover, the structure of the current HIPAA training program, ability to track training, and the need for additional measures in order to reduce the risk of privacy and security violations.

Our review shows that LAC+USC management, and specifically their Privacy Officer, has a good understanding of the HIPAA Privacy Rule regulations and standards. As a result, LAC+USC's compliance program and decision making process regarding implementation of HIPAA and the HITECH Act have benefited.

We request that DHS and LAC+USC management provide a corrective action plan or implement our recommendations within 120 days of this report. We appreciate the opportunity to review the LAC+USC campus and provide recommendations for continued HIPAA and HITECH Act compliance. We also wish to thank HSA and LAC+USC staff who participated in the review for their cooperation.

Please call me if you have any questions, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

WLW:RGC:GZ:LTM

c: William T Fujioka, Chief Executive Officer
Loreto M. Maldonado, Manager, Chief Executive Office
Gregory Polk, Administrative Deputy, Department of Health Services
Robert Pittman, Chief Information Security Officer, Chief Information Office
Stephanie Reagan, Principal Deputy County Counsel, County Counsel
Eva Vera-Morrow, Principal Deputy County Counsel, County Counsel
Audit Committee
Health Deputies